Remarks

Applicants respectfully request reconsideration of the present U.S. Patent application as amended herein. No claims have been amended or canceled. Claims 23 and 24 have been added. Thus, claims 1-24 are pending.

35 USC §103

Claims 1-22 stand rejected as being obvious over Shi (US Patent No. 5,875,296) in view of Shrader (US Patent No. 6,74,359). Applicants traverse the rejections as discussed below.

Various recited embodiments concern providing an ability to de-authenticate (e.g., remove authentication) from a browser that has previously authenticated to a web resource. As discussed throughout the patent specification, a conventional browser user-id and password combination such as used by Shi results in an authentication that ***does not expire*** unless the browser session is terminated. The Office asserts Shi provides various aspects of claimed embodiments. Applicants have **not** analyzed the accuracy of these assertions because the issue is mooted by the failings of Shrader. However, Applicants agree with the Office that Shi fails to teach claim 1's recited:

> accessing a logout resource in the **first** security realm, said logout resource configured to automatically authenticate with a **second** security realm on accessing thereof.

Emphasis added. The Office points to Shrader at col. 8 lines 4-32 as teaching this limitation of claim 1. This is incorrect.

As is well known, e.g., see Uniform Resource Locator (URL) http:// httpd-apache-org/docs/howto/auth-html (to prevent inadvertent hyperlinks, periods in the preceding

URL were replaced with hyphens), if a resource has been protected using "basic authentication," web servers send an "Authentication Required" response to an accessing client browser to let the browser know credentials must be supplied to gain access. On receiving the authentication requirement, the browser, if it supports basic authentication, asks a user to supply a username and password to be sent to the server. If the username and password are correct, the resource will be returned to the browser. Because the HTTP protocol is **stateless**, each access attempt is treated in the same way, even if from the same client, hence the browser caches the credentials and automatically provides them for subsequent accesses. As discussed in the Background section of the Specification at pages 2-3, web browsers do not provide for stopping the caching of the credentials.

Shrader does not teach or even remotely suggest solving the credential caching problem as recited. Shrader notes the problem credential caching problem at col. 1 lines 50-55, continues on to state there is a need to overcome this problem, and then outlines in its Summary that way to overcome the limitation is to use a cookie based credential management that introduces state into the stateless HTTP protocol (see also Shrader at col. 4 lines 35-37 "cookies...track...state"). Rather than accessing a second security realm as recited to invalidate authentication credentials, instead, in the Shrader system, when one seeks to logout, "Web server CGIs" construct "a zero (or null) value...cookie" that removes authentication information previously present.

There is no teaching in Shrader of accessing a second security realm as recited. In fact, since the same cookie is used to store credentials and then lack of credentials, **Shrader teaches away** from recited embodiments since Shrader requires modifying **the same resource** (the cookie). There is no teaching or suggestion of the recited "accessing a logout resource...configured to automatically authenticate with a second security realm on accessing thereof."

Consequently, it is respectfully submitted that the suggested combination of Shi and Shrader is unworkable, and these references, whether considered individually or one in view of the other, fail to render the claim 1 embodiment obvious. Because related limitations are present in independent claims 6, 10, 15, 19, and 21, the suggested combination also fails for at least the reasons discussed above for claim 1.

Further, regarding independent claims 6, 15, and 21, these claims recite a basic authentication context. As discussed above cookies are **not** part of basic authentication and consequently the documents relied on by the Office can not teach or even remotely suggest the claimed embodiments!

Regarding dependent claims 2-5, 7-9, 11-14, 16-18, 20, and 22, while these claims introduce additional limitations further distinguishing from the documents relied on by the Office, the specific rejections of these claims are not being evaluated at this time in order to focus attention on the allowability of the independent claims. However, it is respectfully submitted that these dependent claims are allowable for at least the reason as depending from allowable base claims.

Further, regarding dependent claims 5 and 14, as with independent claims 6, 15, and 21, these dependent claims these claims also recite a basic authentication context. As discussed above the cookies used in the documents relied on by the Office are **not** part of basic authentication and consequently the relied on by the Office can not teach or even remotely suggest the claimed embodiments!

New claims 23 and 24 are allowable for at least the reasons discussed above.

Conclusion

For at least the foregoing reasons, Applicants submit that the rejections have been overcome. Therefore, claims 1-24 are in condition for allowance and such action is earnestly solicited.

The Examiner is respectfully requested to contact the undersigned by telephone to discuss this matter if the foregoing is not deemed persuasive.

Please charge any shortages and credit any overcharges to our Deposit Account number 02-2666.

Respectfully submitted,

Date: November 1, 2004

Steven D. Yates
Patent Attorney
Intel Corporation
Registration No. 42,242
(503) 264-6589

c/o Blakely, Sokoloff, Taylor & Zafman, LLP
12400 Wilshire Boulevard
Seventh Floor
Los Angeles, CA 90025-1026